

Week – 3

Vulnerability Scan Report

Tool Used: Nessus Essentials

Scan Target: 127.0.0.1 (Localhost)

Date: August 8, 2025

Tools Used

- **Nessus Essentials**
 - **Scan Target:** 127.0.0.1 (localhost)
 - **Platform:** Browser-based Nessus Dashboard
-

Step-by-Step Scan Process

1. Downloading Nessus Essentials

- Visited the **official Tenable Nessus download page**: <https://www.tenable.com/downloads/nessus>
 - Selected the appropriate installer based on the system architecture (Windows in this case).
 - Chose **Nessus Essentials** version – free for personal or academic use.
-

2. Installing Nessus

- Launched the downloaded .exe installer.
 - Followed the step-by-step **GUI-based installation wizard**:
 - Accepted the license agreement
 - Selected installation location (default: C:\Program Files\Tenable\Nessus)
 - Waited for Nessus to install required services (takes 3–5 minutes)
 - Once complete, Nessus automatically **launched in the default browser** using: <https://localhost:8834/>
-

3. Activating Nessus Essentials

- Chose "**Nessus Essentials**" from the activation options on the browser page.
 - Entered my **name and email address** to receive a **free activation code** from Tenable via email.
 - Entered the received **activation code** into the browser.
 - Nessus began **downloading the necessary plugins** (first-time setup may take 15–20 minutes).
-

4. Creating a New Scan

Once plugin installation was complete:





- Clicked "**New Scan**" from the Nessus dashboard.
 - Chose the "**Basic Network Scan**" template.
 - In the scan configuration:
 - Entered a name (e.g., *Localhost Vulnerability Scan*)
 - Set the **target IP address** to 127.0.0.1 (the local machine)
 - Left advanced settings at default
 - Saved the scan and clicked "**Launch**" to start scanning.
-

5. Scanning Process

- Nessus performed a comprehensive scan of the system:
 - Scanned for **open ports, services, operating system, and software vulnerabilities**
 - Checked for **insecure protocols, default configurations, and known exploits**
 - Compared findings against its regularly updated **vulnerability database**
 - The scan duration depended on system resources – approximately **5–10 minutes** for localhost.
-

6. Viewing and Analyzing Results

After scan completion:

- Clicked the scan name to open the **Scan Report Dashboard**
 - Nessus presented results categorized by **severity**:
 -  **High**
 -  **Medium**
 -  **Low**
 -  **Info**
 - Hovered over each vulnerability to view:
 - Detailed **description of the issue**
 - **CVSS score** (severity)
 - **Affected ports/services**
 - **Solution or remediation suggestions**
-

7. Sample Vulnerabilities Found

- **TLS/SSL Supports Weak Cipher Suites (High)**
 - Indicates that the system supports outdated/weak encryption methods
 - Could lead to encrypted traffic being intercepted and decrypted
- **SMB Signing Not Required (High)**
 - SMB traffic could be intercepted or altered
 - Should enable **SMB message signing** to ensure message integrity
- **Outdated Software Detected (Medium/Low)**
 - Software versions with known vulnerabilities still installed

8. Exporting Results

- Nessus allows exporting the full scan report in various formats:
 - **PDF**, **CSV**, or **HTML**
- From the scan results page, selected **“Export”** → **“PDF”** to save a copy of the scan report.

Conclusion

The Nessus vulnerability scan successfully identified critical and high-risk issues on the localhost system. These findings are valuable for strengthening the host's security posture. By reviewing the report and applying the recommended remediations, system vulnerabilities can be significantly reduced or eliminated.